Response of the European Criminal Bar Association
to the EU Comission's Consultation on the AI Act

The ECBA

The European Criminal Bar Association ('ECBA') was founded in 1997 and is an association of independent specialist defence lawyers across Europe, representing the views of defence lawyers and promoting the administration of justice and human rights under the rule of law in Europe and among the peoples of the world.

The ECBA is one of the main interlocutors of the European institutions on issues of criminal justice and the protection of the right of defence and fundamental rights, representing thousands of legal practitioners all around Europe through their direct affiliation to the Association as individual members, or through the Collective members that participate to the life of the Association.

The ECBA acknowledges the growing role of technology in criminal law and criminal procedure, the current digitalisation of justice and the many other rapid developments in this domain, e.g. the rise of AI, digital evidence, the role of encryption in communication and financial flows and the use of video connections in court procedures or for remote communication. These developments must comply with the right to privacy and non-discrimination, procedural safeguards and must have sufficient effective legal remedies. Due to the rapid development in the technical field, the ECBA also considers it important that lawyers have knowledge in this area and that our members can exchange experiences from the various Member States and learn from them.

The European Commission sent an invitation for consultation on the Commission Guidelines on the application of the *definition of an AI system* and the *prohibited AI practices* established in the AI Act (Regulation (EU) 2024/1689).

Taking into consideration the scope of ECBA's activities, this response to the EU Commission's consultation will refer only to aspects relevant to substantive or procedural criminal law.

EUROPEAN CRIMINAL BAR ASSOCIATION
An association of European defence lawyers

Table of Contents

I. DEFINITION OF AI SYSTEM

An Artificial intelligence system (AI system) is defined in Article 3 (1) of AI Act as

> 'a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments'.

Recital 12 is relevant for this definition, which provides some additional context. Based on this Recital we could argue that the legal definition provided under Article 3 (1) of AI Act focuses on the following:

- Ensuring legal certainty. From a criminal law perspective this should align with the principle of legality.
- Developing key characteristics of AI systems necessary to distinguish them from simpler traditional software systems or programming approaches. In this regard, the Recital provides several key characteristics of AI systems: being a machine-based system; its capability to infer (through machine learning, logic- and knowledge-based approaches); the capability to generate outputs for explicit or implicit objectives that influence physical or virtual environments; the capability of operating with varying levels of autonomy (meaning some degree of independence of actions from human involvement); and adaptiveness after deployment through self-learning capabilities.
- Providing flexibility to accommodate any future technological developments in the field.

When comparing the key characteristics found in Recital 12 with the criteria specified in the definition of AI systems, it appears that future European Commission Guidelines should

emphasize each criterion and provide examples that differentiate AI systems from traditional software systems or programming approaches.

In this regard, the phrase 'may exhibit adaptiveness after deployment' should be clarified to emphasize the system's self-learning capabilities after deployment, particularly its ability to change without human intervention. Additionally, it should be emphasized that the system can process input from both human and non-human sources.

Regarding substantive and procedural criminal law, a key concern is the relationship between the AI system definition and other legal definitions at the European or international level: 'computer system' (Article 1(a) of Cybercrime Convention), 'information system' (Article 2(a) of Directive 2013/40/EU), and 'information and communications technology system' (Article 2(a) of the United Nations Convention against Cybercrime).

> **Cybercrime Convention**
>
> ‚Computer system' means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.
>
> **Directive 2013/40/EU**
>
> 'Information system' means a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.
>
> **United Nations Convention against Cybercrime**
>
> ‚Information and communications technology system' shall mean any device or group of interconnected or related devices, one or more of which, pursuant to a program, gathers, stores and performs automatic processing of electronic data.

While Recital 12 clearly distinguishes AI systems from traditional software systems, it must be acknowledged that AI systems can simultaneously fall within the scope of one or more of these established definitions, creating potential overlaps in legal application.

From a substantive criminal law perspective, it is essential to clarify whether established cybercrimes (illegal access, illegal system interference, illegal interception, computer-related fraud, etc.) apply to AI systems. Similarly, when discussing search and seizure of stored computer data, it is crucial to analyse how AI systems logically interact with computer systems, information systems, and data storage media, as this may affect both investigative procedures and evidence collection.

Although these topics exceed the scope of the AI Act, the interpretation of the AI systems' definition remains crucial. In this regard, one concern could be the term ‚machine-based', which under Recital 12 refers to the fact that AI system runs on machines.

As we can see from the definitions provided under the previously mentioned legal instruments, the preferred terminology is device or a group of interconnected or related devices. In this regard, it would be preferable to emphasize that machine-based can encompass a device or a group of interconnected or related devices part of a computer or information system as defined in Article 1(a) of Cybercrime Convention, Article 2(a) of Directive 2013/40/EU, and Article 2(a) of the United Nations Convention against Cybercrime. It would also be preferable to clarify if 'machine-based' includes a decentralized system powered by blockchain technology or DLT (as defined in the MiCA Regulation).

Furthermore, it remains unclear whether investigative tools like Sweetie 2.0, used by law enforcement, qualify as AI systems under the Act. The phrase 'designed to operate with varying levels of autonomy' lacks sufficient clarity for this determination.

Even when applying the key characteristics of AI systems from Recital 12, uncertainty persists about whether such investigative bots demonstrate sufficient autonomy and independence from human involvement to fall within the definition's scope. In this regard, the European Commission Guidelines should establish clear criteria regarding autonomy thresholds to ensure consistent application of the definition. It may be relevant to offer clear examples to make a distinction between full human control, partial autonomy, high autonomy and full autonomy.

II. PROHIBITED AI PRACTICES

a) Article 5 para. 1 (a) AI Act

> 'the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm'.

Firstly, it remains unclear whether this prohibition covers investigative tools like Sweetie 2.0 when used by law enforcement for gathering intelligence or evidence in criminal proceedings. From the first reading, it seems that the Article is primarily aimed at commercial AI systems that are used to manipulate consumers or private individuals, without restricting the use of such systems by law enforcement bodies.

Nonetheless, Article 5 para. 1(a) does not explicitly exempt law enforcement. If law enforcement are to be allowed use investigative tools like Sweetie 2.0 there should be explicit guidance regarding deceptive techniques in law enforcement investigations which complies with fundamental rights' standards.

b) Article 5 para. 1 (h) and para. 2-8 of the AI Act

The AI Act establishes several procedural safeguards for real-time remote biometric identification systems in law enforcement contexts, balancing operational needs with fundamental rights protection. However, several areas require clarification:

- It would be preferable to provide examples of what biometric identification consists of and clarify if digital biometrics are covered by the provision. For instance, facial patterns, fingerprints, voice characteristics, digital behaviour patterns, avatar recognition in Metaverse, etc.
- It would be preferable to provide examples relevant to understanding the phrase 'publicly accessible spaces' and take into consideration the distinction between the physical space and Metaverse.
- There are no criteria to assess a 'duly justified situation of urgency', which could lead to an overbroad exception. Exceptions need to be clearly limited and strcitly defined by law.
- It should be made clear that para. 8 also refers to the Law Enforcement Directive (LED) 2016/680 regarding data protection in criminal matters.

12 January 2025

Rapporteur:
George Zlati (Romania)

ECBA Cyber & AI Working Group:

Alexis Anagnostakis (WG Co-Chair, Greece)
Gwen Jansen - de Wolf (WG Co-Chair, the Netherlands)
Adrian Sandru (Romania)
Amedeo Barletta (Italy)
Federico Cappelletti (Italy)
Julian Hayes (United Kingdom)
Marie Poirot (France)
Stefanie Schott (Germany)
Vânia Costa Ramos (Portugal)